**3GPP TSG-SA3 Meeting #102Bis-e *draft\_S3-211044-r2***

**e-meeting, 1 - 5 March 2021** Revision of S3-20xxxx

**Source: Ericsson**

**Title: High-level conclusions to KI#4 "Securing initial access for UE onboarding between UE and SNPN"**

**Document for: Approval**

**Agenda Item: 2.12**

# 1 Decision/action requested

***It is proposed to add the conclusions to TR 33.857 [1].***

2 References

[1] 3GPP TR 33.857 "Study on enhanced security support for Non-Public Networks (NPN)"

# 3 Rationale

## 3.1 Introduction

This contribution proposes high-level conclusions to Key Issue #4 "Securing initial access for UE onboarding between UE and SNPN".

## 3.2 Type of authentication procedure

Most of the solutions to Key Issue #4 (Solutions #8, #9, #10, #11, #12, #14, #15, one variant of #16) suggest basing the authentication procedure for securing initial access on the primary authentication procedure. This has the advantage that existing security measures like NAS and AS security building on primary authentication procedure can be used.

## 3.3 Entities involved in the authentication procedure

Most of the solutions to Key Issue #4 (Solutions #8, #10, #11, #12, #15, #16) propose that the DCS acts as authentication server and AUSF as pass-through authenticator. This has the advantage that the primary authentication procedure can be reused with the enhancement that the DCS performs the actual authentication with the UE.

## 3.4 Credentials pre-provisioned in the UE and the DCS

Several solutions to Key Issue #4 (Solution #8, #10, #11, variant of #16) describe solutions where only default credentials for mutual authentication between UE and DCS need to be pre-provisioned in the UE and the DCS, no onboarding SNPN credentials. This has the advantage that there does not need to be any kind of earlier relationship of the UE to the onboarding SNPN before the onboarding is started.

## 3.5 Relationship to Key Issue #1 "Credentials owned by an external entity"

Most of the solutions to Key Issue #4 (Solutions #8, #10, #11, #12, #15) describe solutions that also are solutions to Key Issue #1, with the DCS as external entity. This has the advantage that procedures can be aligned between Key Issues #1 and #4, the standardization and implementation impact is reduced.

## 3.6 Format of the identifier for the default credentials

Most of the solutions to Key Issue #4 (Solutions #8, #9, #10, #11, #12, #15, one variant of #16) propose that the UE identifiers contained in the default credentials and used during initial access are SUPI and SUCI. It can hence be concluded that the UE identifier in the default credentials has the same format as a SUPI of type NSI, i.e. it is a NAI.

# 4 Detailed proposal

\*\*\* BEGIN CHANGES \*\*\*

## 7.x Conclusions on KI #4: Securing initial access for UE onboarding between UE and SNPN

In case that security for initial access for UE onboarding between UE and SNPN is based on the primary authentication procedure with mutual authentication, the following is concluded:

- Primary authentication using any key-generating EAP-method is enhanced to support the usage of the DCS as authentication server and an enhanced AUSF as pass-through authenticator.

* When the DCS supports key deriving EAP method, the enhanced AUSF uses the MSK received from the DCS to derive the necessary 5G keys (e.g., KAUSF, KSEAF).

- The authentication is based on default credentials pre-provisioned in the UE and DCS providing mutual authentication between UE and the DCS.

- Key material generated from the enhanced primary authentication procedure is used to establish the KAUSF and further keys in the 5G key hierarchy as specified in TS 33.501 [2].

Editor's Note: Further conclusions are ffs, including whether initial access can be allowed without mutual authentication as primary authentication.

\*\*\* END CHANGES \*\*\*